Abstract

A sequence generator for generating a pseudo random sequence for random number generation or a stream cipher engine includes a plurality of linear feedback shift registers operable to generate a plurality of binary sequences. A plurality of nonlinear functions having the binary sequences as their input and operable to generate a second plurality of binary sequences. There are at least two switches and a controller including a shift register operable to control said first and second switches. The first switch is operative to select one of the second plurality of binary sequences to the first bit of the shift register, and the second switch is operative to select one of said second plurality of binary sequences to the output of the sequence generator.